Blockchain in the Smart City

Participation and democratic Involvement

Lasse Berntzen

University of South-Eastern Norway

Keynote presentation

IARIA DIGITAL 2021

November 14th-18th, Athens, Greece

About myself

- Professor in Information Systems at the University of South-Eastern Norway
- Done research on e-democracy and e-government since 2004
- Shifted focus to Smart Cities in 2015
- Since 2019 I have implemented blockchain solutions for a smart energy project (Smart-MLA)

Introduction

Blockchain is often mentioned as a promising technology for new inventions.

The purpose of this keynote presentation is to discuss the potential of using blockchain for participation and democratic involvement in smart cities.

Smart city definition #1

"A smart city is a well defined geographical area, in which high technologies such as ICT, logistic, energy production, and so on, cooperate to create benefits for citizens in terms of well being, *inclusion* and *participation*, environmental quality, intelligent development; it is governed by a well defined pool of subjects, able to state the rules and policy for the city government and development"

R. P. Dameri, "Searching for Smart City definition: a comprehensive proposal," International Journal of Computers and Technology, 11(5), pp. 2544-2551, 2013.

Smart city definition #2

*"Projects of smart cities have an impact on the **quality of life** of citizens and aim to foster more informed, educated, and participatory citizens.*

*Additionally, smart cities initiatives allow members of the city to **participate** in the governance and management of the city and become active users"*

Chourabi et al. "Understanding Smart Cities: An Integrative Framework, Proc. 45th Hawaii International Conference on Systems Sciences, pp. 2289-2297, 2012

Smart cities

Smart cities is a concept with many definitions.

Most definitions includes the use of computer technology

Main objective is to improve quality of life for its citizens

- Provide better services
- Reduce environmental footprint

The two definitions shown in the previous slides emphasize **participation** as important.

Participation and democratic involvement

Polling

Voting

Consultations

Petitions/ citizen initiatives

The blockchain

Blockchain is a *decentralized, immutable, distributed ledger*.

Essentially, blockchain makes it possible to do transactions without an intermediary.

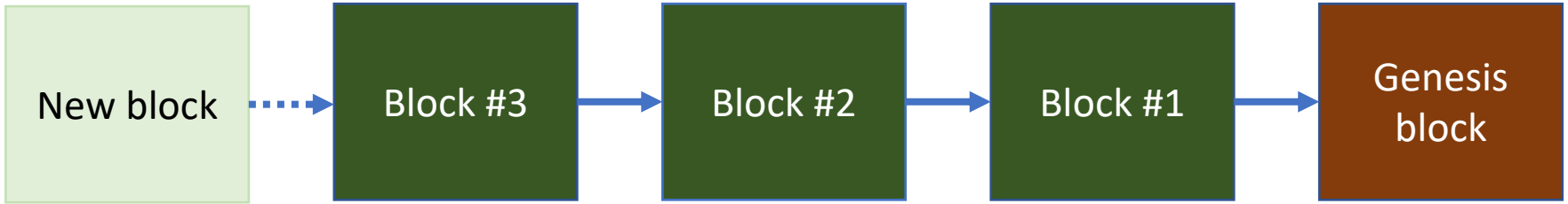
Blockchain basics

A blockchain consists of blocks chained together.

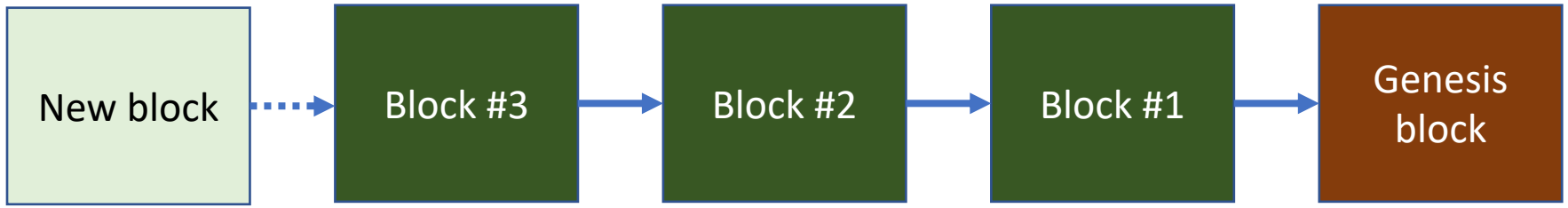
The blocks are timestamped and linked to the prevoius block in the blockchain using cryptographic techniques.

This secures the integrity of the blockchain.

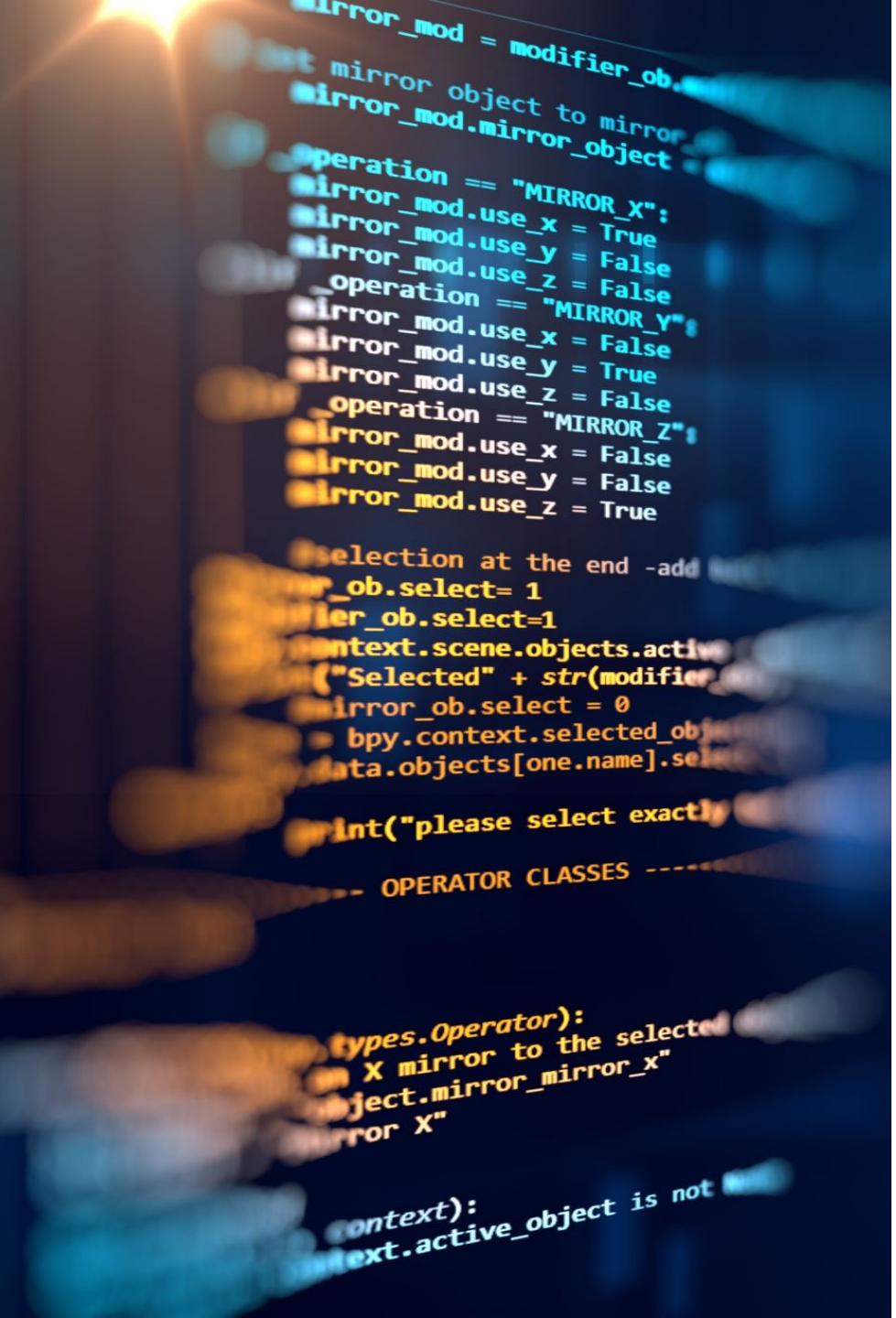
A change to one block in the blockchain will make the whole blockchain invalid.



Blockchain basics

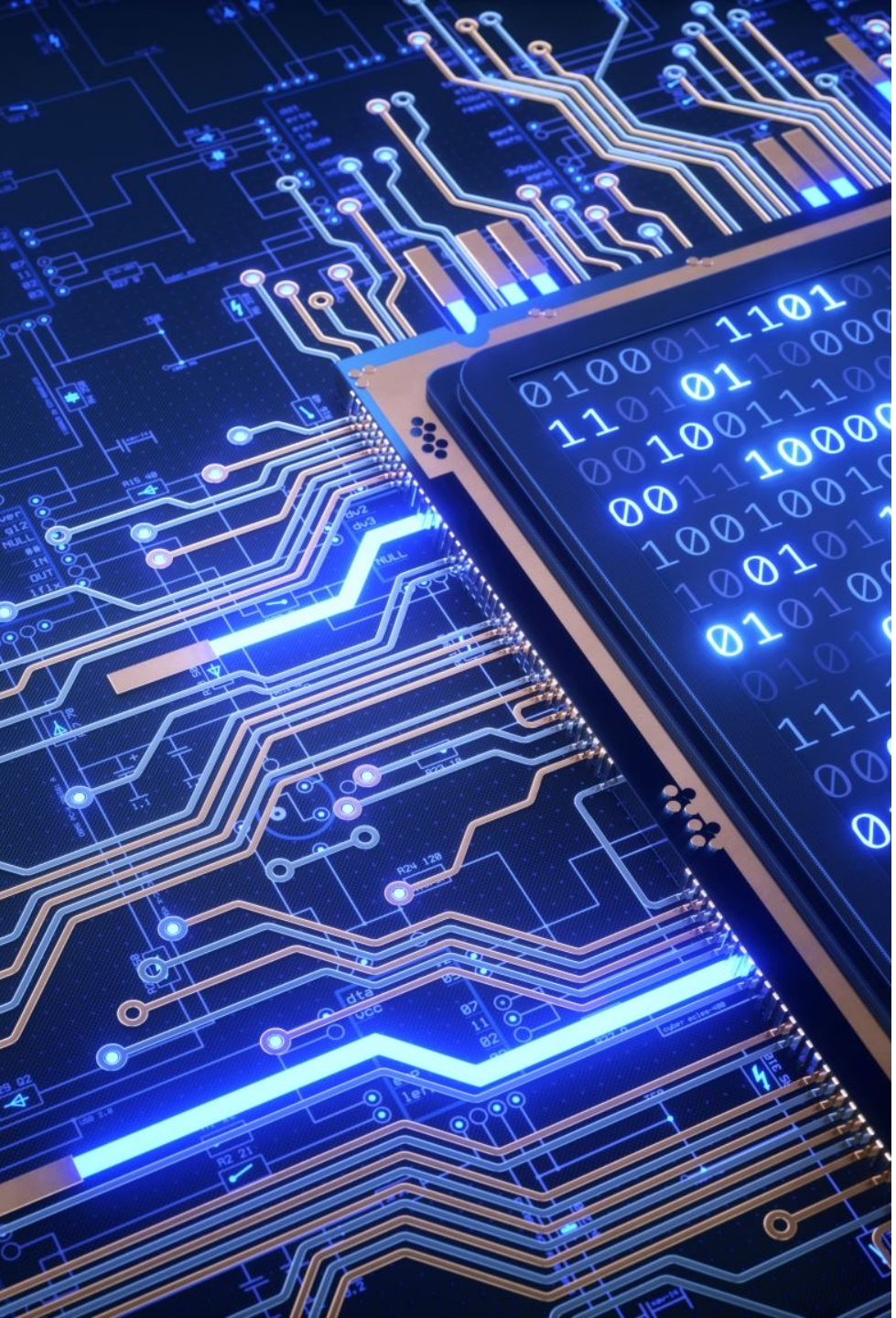


- Each block contains a link to the previous block
- Each block contains the hash value of the previous block
- Each block is encrypted (including the hash value of the previous block)
- Changes to one block will make the whole blockchain invalid (for one node)



Blockchain basics

- First, transactions are validated.
- A block is built from the transactions.
- Validation of a block on a public blockchain (Bitcoin or Ethereum) requires solving a complex mathematical problem using computing resources (proof of work).
- Miners do this work.
- The miner that first validates a new block receives a cryptocurrency reward for the work performed.



Blockchain basics

- A blockchain copy is maintained by a **node** (a computer)
- All nodes are connected to other nodes in the network
- The Ethereum blockchain consists of thousands of nodes
- A node broadcasts transactions and blocks to the network and receives transactions and blocks from the network
- The node synchronizes the state of the blockchain with the rest of the nodes
- If a blockchain on a node is hacked, it becomes invalid, and the node will replace it with a valid copy from another node.

Proof of work

After validation, the block is submitted to all nodes in the network.

Each node add the block to its own blockchain.

Acceptance of blocks are based on majority consensus between the nodes

So, theoretically, a blockchain can be compromised by someone controlling more than half of the nodes.

But this is highly unlikely.

Distributed ledger

Each node processes and stores an identical copy of the latest version of the ledger (blockchain).

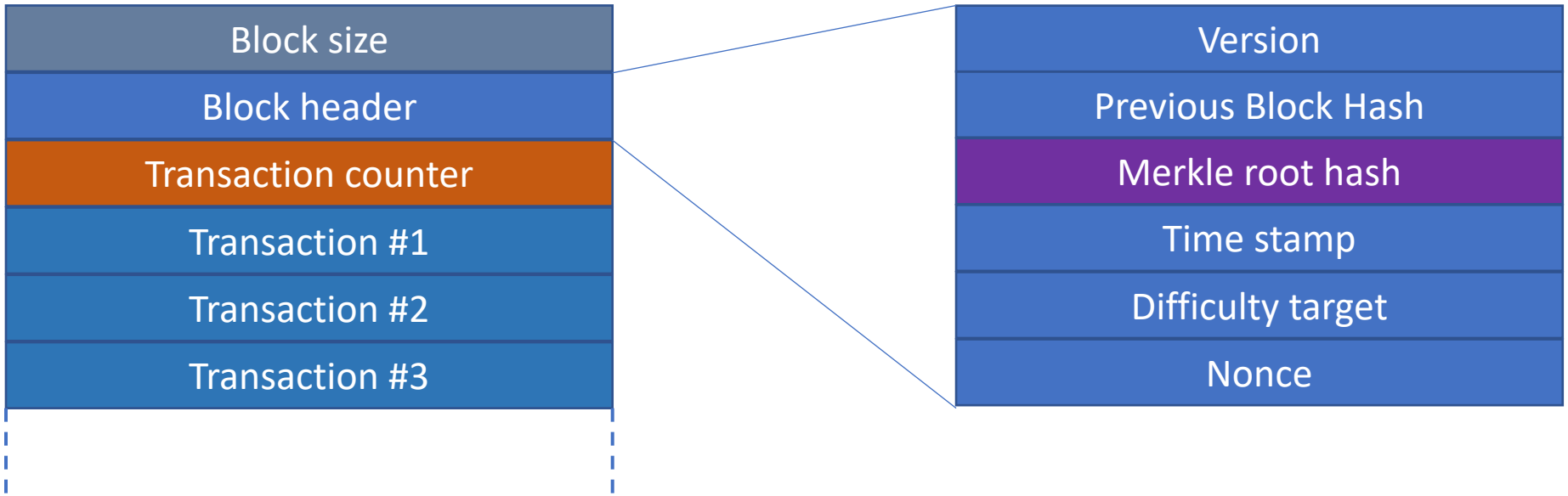
Updates are performed independently and recorded by every node in the network.

The nodes then execute a voting process on the validity of the new update.

When consensus is reached (a majority of nodes votes yes) the block is added to the ledger.

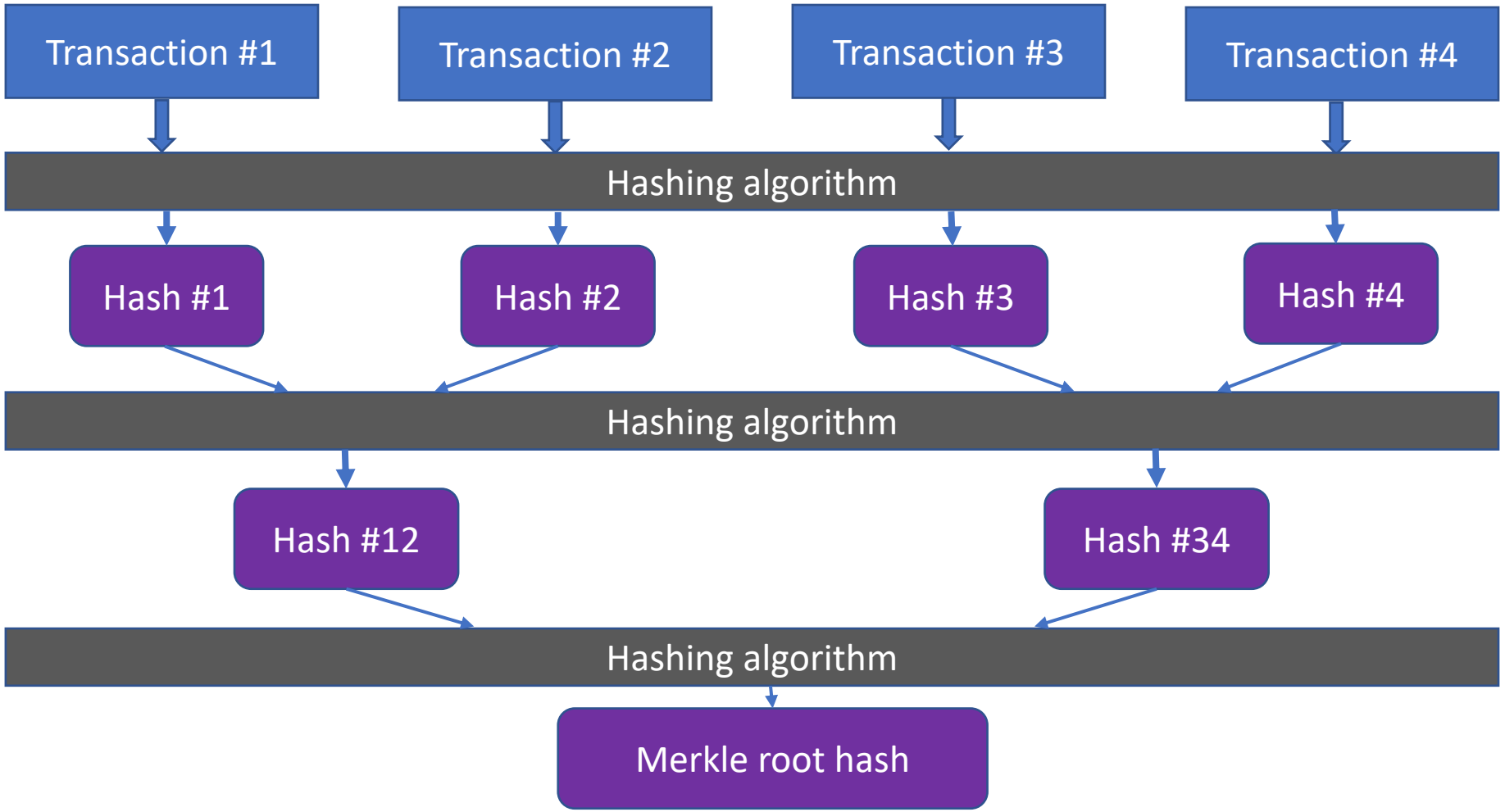
Therefore, a possible attack on a minority of the nodes will be rejected.

Blockchain blocks and block header



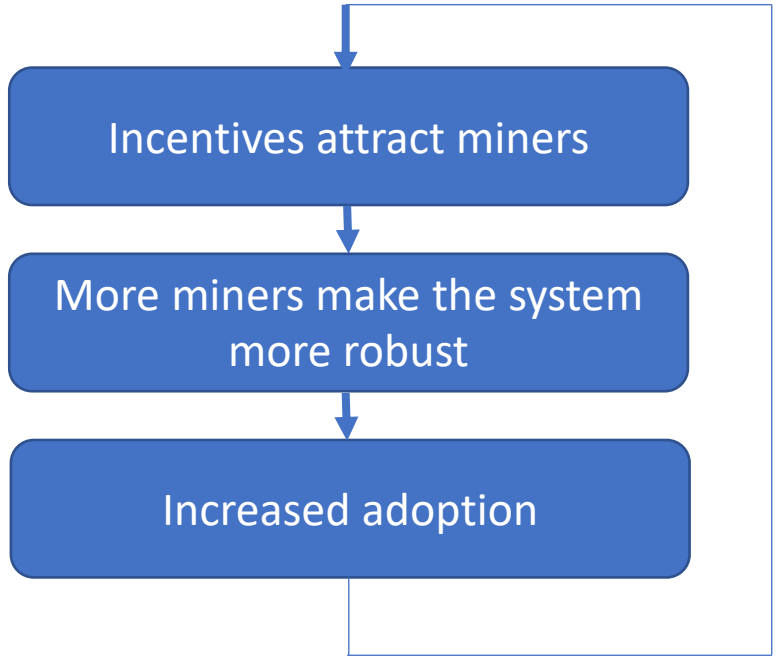
The Merkle tree (see next slide) ensures the integrity of each transaction added to a block

Computing the Merkle root hash

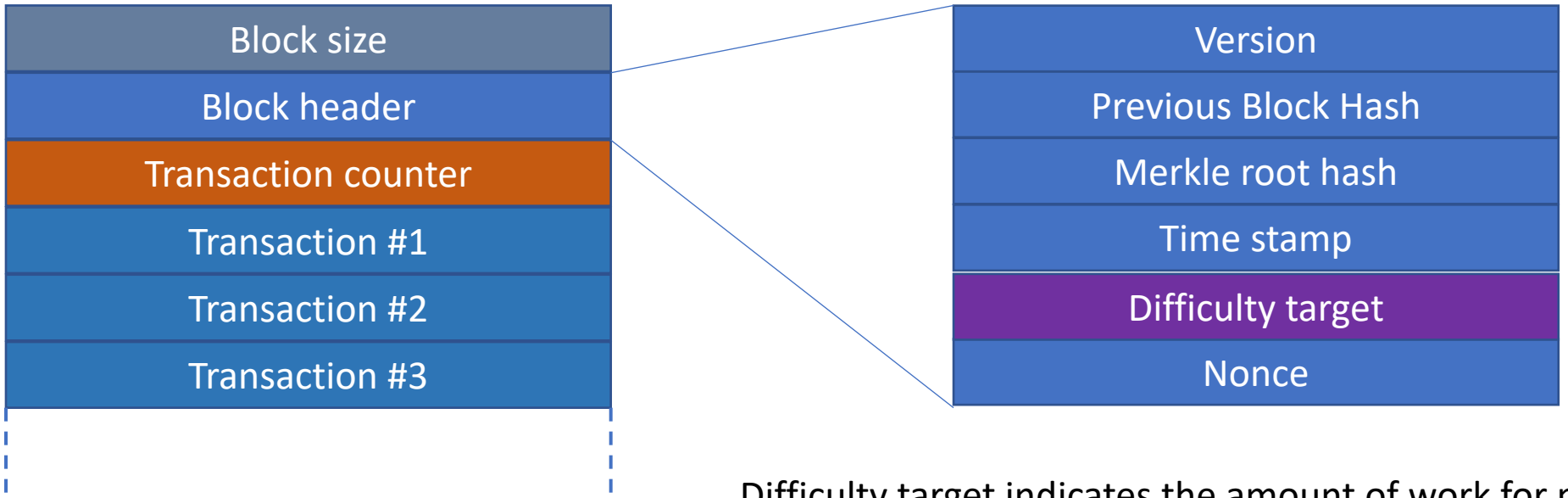


More about miners and complexity

- Miners validate the blockchain
- The miner that first succeeds to solve the mathematical problem is awarded (with cryptocurrency)
- Faster CPUs / GPUs / ASICs reduce the time to solve problems. Bitcoin network responds by increasing the difficulty of the mathematical problem.
- Mining pools are a way to consolidate individual resources to solve more problems and get awarded.

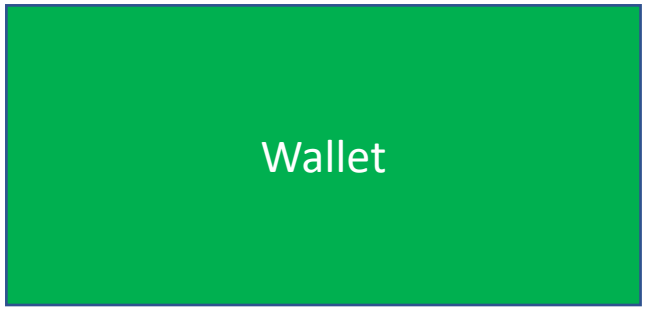


Blockchain blocks and block header



Difficulty target indicates the amount of work for mining

The Wallet



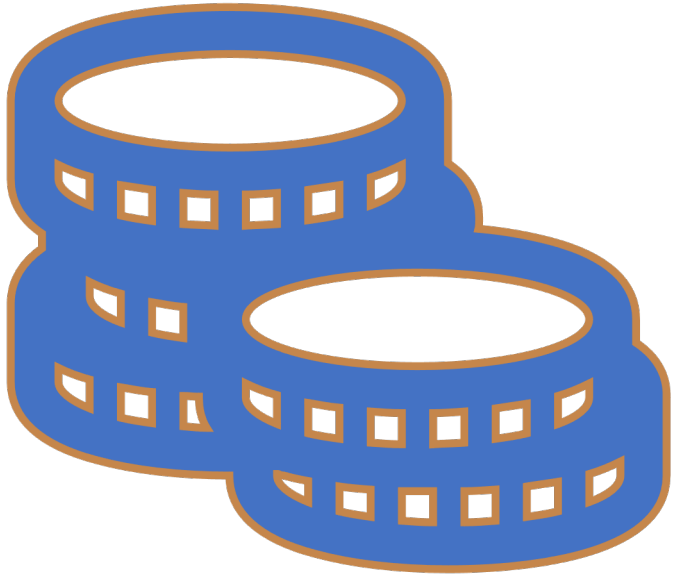
The wallet is used for sending, receiving, and storing cryptocurrency.

Similar to a bank account.

- Different types:
  - Online (software) wallets
  - Physical (hardware) wallets (e.g., USB-stick or even paper)
- The wallet is needed for paying for transactions.

Exchanges

- An exchange converts between currencies and cryptocurrencies.
- Example: CoinBase
- Necessary to do transactions on the public (no test) blockchains



Public blockchain

A blockchain may be **public** or **private**.

Everyone has access to a public blockchain and can examine the transactions that have been made.

Everyone can add to the blockchain (but a fee is required). It is a global infrastructure.

Transaction fee is based on supply/demand. Payment may be exchanged into real currency.

The blockchain is semi-anonymous; the user is identified with a binary address.

Private blockchain

In a private blockchain the situation is different. A private blockchain may require permission to add to and examine the content of the blockchain.

Only approved nodes can submit new blocks to the blockchain

The private blockchain has a limited number of nodes and is owned by a company or organization. Users pay for transactions, but payment has no real value

The private blockchain does not use proof of work.

So, security relies on authentication of the submitters

Ethereum

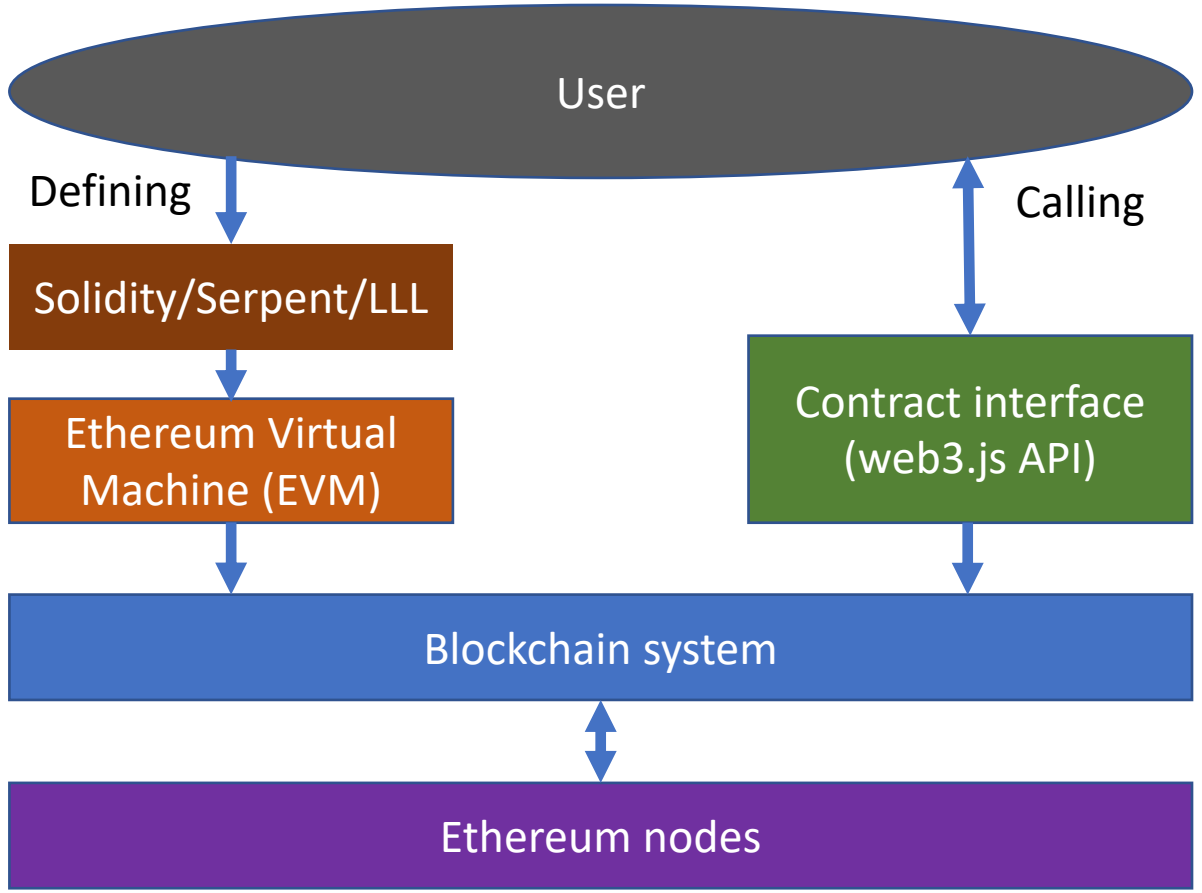
- Ethereum is an open-source blockchain platform with excellent support for writing smart contracts.
- A smart contract is a computer program that is automatically executed when certain predetermined conditions are met.
- Code is normally written using the Solidity programming language on top of the Ethereum platform. Solidity has a syntax close to JavaScript.
- Smart contracts facilitate storing and retrieving transaction information in the Ethereum blockchain.
- Smart contracts are autonomous and distributed.

Ethereum architecture

The figure shows the development and use of smart contracts.

The smart contract is written in a programming language, e.g., Solidity and written to the blockchain.

The smart contract is executed through an API, e.g., web3.js



Two types of participation

Political participation

- Polling
- Consultations
- Voting
- Petitions

Non-political participation

- Citizens as sensors
- Digital planning

Political participation

- Political participation is about influence.
- The city can initiate participation:
  - Polling
  - Voting
  - Consultations
- Participation can be initated by the citizen:
  - Petitions / citizen initiatives

Polling

- The city uses polling to seek opinons on issues.
- Polling is done on a sample of citizens.
- Polling is not binding.
- Results may be published or not.

Voting

- Voting is a process where all eligible citizens are invited to cast their votes (in some countries attendance is mandatory).
- The candidate or proposal that receives the majority of votes win the vote.
- Voting may be advisory or binding:
  - Advisory – politicians decide after seeing the results.
  - Binding – the citizens decide.

Consultations

- In a consultation, the citizen is asked for his/her opinion on an issue.
- The city, not the citizen, initiates the consultation.
- The opinion is used as input for decision making, and the city decides the weight of the specific opinion.
- For the citizen, feedback may be seen as important.

Petitions or citizen initiatives

- Petitions or citizen initiatives can be submitted by a citizen or a group of citizens.
- The petition or citizen initiative asks the city to do something about a specific issue.
- It is often a requirement of a specific number of signatures to be effective.
- Also, it is often regulated that the appropriate body needs to discuss the issue within a certain timeframe.
- But no guaranteed about success is guaranteed.

Non-political participation

Citizens as sensors

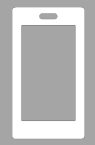
Citizens make their own observations and reports them to the city

Digital planning

Citizens can voice their opinions on public planning processes

Citizens as sensors

A “**human sensor**” is a person that observes some issue and reports it using some platform.



Smart phones

Webpages

Dedicated wearables

Other forms of participation in smart cities

Political bodies use of meeting technology

Requests and complaints

Meeting technology

New technology is also employed in meetings of political bodies:

- Webcasting of meetings
- Voting
- Submit proposals
- Ask permission to speak

Requests and complaints

Another area is requests and complaints

Put it on the record so everyone knows it has been submittet

Challenges and limitations of using blockchain

Generally, private blockchains are less expensive to use, but also less secure since the infrastructure is controlled by an owner.

The public blockchain is better suited for democratic purposes since the the public domain may increase the trust.

Longer entries, e.g., documents can be stored in a database, with some kind of notary function being done by the blockchain

Polling

- Registering the poll results on the blockchain can improve transparency and make sure the poll is not tampered with.
- The cost/benefit of using a public blockchain for this purpose may be low, due to the transaction fees on public blockchains.

Voting

- Registering votes on the blockchain has several advantages.
- Make sure that votes are not tampered with.
- Improved transparency.
- Anonymity is easy to implement while making sure that each person only can cast on vote.
- The costs may be prohibitive, but the importance of the above may justify the costs.

Consultations

- The answers to consultations may be long.
- Blockchain can be used as a notary function registering the submission of responses together with a hash of the document to prevent tampering.
- Transaction costs in a public blockchain will be acceptable, since the number of responses are low (compared to voting and polling), and the impact is high (often valuable input).

Petitions

Petitions or citizen initiatives may be well suited for blockchain use. The petition or citizen initiative itself can be stored on the blockchain

Signatures supporting the petition or citizen initiative may also be stored on the blockchain, and can be used to ensure no-tampering of the signatures

Citizens as sensors

Registration of the report made to the authorities ensures both transparency and accountability.

A typical example of a reporting application is FixMyStreet.com.

Blockchain could be used to ensure transparency, but also accountability.

Everyone can see when the report was filed (transparency)

And when the respective authority did something (accountability)

Digital planning

Digital planning is a form of a consultation, but it is focused on stakeholder interests in local and regional planning processes.

In Norway, the application **digital planning dialog** integrates a geographic information system with a electronic document handling systems.

The application aims to make communication between stakeholders easier and more transparent.

Blockchain could increase transparency and make sure submitted opinions are not lost.

Conclusions and Future Work

- The purpose of this keynote presentation was to draw attention to the possible use of blockchain for participation and democratic involvement.

Conclusions

A public blockchain implements a *decentralized*, *immutable, distributed ledger*.

Adoption of applications supporting participation and electronic involvement depends on trust among the citizens.

The public blockchain may be used to enhance trust, since the blockchain is transparent, with no owner, and srong mechanisms preventing record tampering.

Conclusion

Lately, Ethereum transaction costs have increased to new heights, with transaction costs of $50 and more.

https://bitinfocharts.com/comparison/ethereum-transactionfees.html#3y

For low numbers and high impact, the cost/benefit may be reasonable, e.g., the submission of answers to consultations or registration of reports from “human sensors”.

But for polling and voting, the cost/benefit may be rather low.

Future Work

Based on our experience with developing Ethereum smart energy applications, we plan to implement a set of demonstrations to show how blockchain can be used with polling, voting, consulting, and petition/citizen initiative applications.

We will also use the thoughts presented here as basis for a paper on blockchain for participation and democratic involvement.

Thank you for your attention

lasse.berntzen@usn.no